肖新光，网名江海客，安天实验室首席技术架构师，研究方向为反病毒和计算机犯罪取证等。

当免费模式遭遇安全价值观

——一个反病毒老兵的复盘与反思

一个关于物种起源的寓言

在互联网时代到来之前，操作系统草原上只奔跑着三类动物，那就是：应用软件、安全软件和恶意代码。请原谅我使用“恶意代码”这个偏学术的名称，因为它能更准确地统称传统感染式病毒、木马、蠕虫等这些有害的代码物种。

我依托如下的脉络，把这些动物进行聚类：应用软件的主要作用是创造应用价值；而恶意代码的设计目的是对应用价值进行侵害；而安全软件是没有应用价值的，它是对安全价值的保障。

用户这个上帝拥有这个草原，后来为了挖掘草原的价值，他又制造了奶牛、绵羊，它们就是应用软件。但上帝心中潜在的少许恶念，也创造了另外一种东西，一些害虫、恶兽，即恶意代码。于是，他又创造了牧羊犬和其他的保护者，来保护草原和其上的有益动物。

一切应用都是要基于操作系统来运行，这对于单机和局域网时代来说必然，但1998年起，这种局面有所不同：当草原上的动物们仰望头顶时，发现自己可以生出翅膀，到达星空，这个星空叫做互联网。

此时，操作系统草原的动物对于草原上的互联网星空有着不同理解。当安全软件认为互联网虽然带来了安全威胁，但也为反病毒软件带来了病毒样本实时上报、病毒库实时派发等应用前景的时候；当传统的商用软件认为互联网带来更多的是一个不依托于包装和渠道的低成本分发方式的时候，一个新的物种即将孕育而生，它就是互联网客户端。互联网客户端，绝不是传统局域网模式下C/S模式中的Client。一个新物种被命名，在于它一定要有自己独特的、不同于其他物种的盈利模式。因此，当时的类似浏览器、邮件工具等基本还只是服务于网络的传统应用软件，还没有演进成真正意义上的互联网客户端。

互联网客户端的本质，在于对它来说每个用户不是一个孤立的Client个体，其相互之间存在关联、共性，同时也可以根据个性聚类。它不仅是用户到达网络内容的通道，更是网络内容个性化传递给用户的平台。海量用户的信息形成一个超级的长尾，在没有收费支撑的情况下，每个免费用户对整个客户端网络的微小贡献，却可以聚合成巨大的商业价值。

而另外一种畸形的物种也在悄然崛起：它们没有在操作系统草原的族群中找到自己的位置，无法与应用软件一样具有完整的用户价值，也没有像恶意代码一样直接破坏用户数据，或窃取用户最核心的账户或虚拟财产；它们给用户带来流量的损失、弹窗的干扰，它们改变搜索引擎的搜索结果以插入自身广告，它们和反病毒产品频繁摩擦，它们窥视用户的使用习惯和痕迹。

从传统的安全分类，它们只是轻安全威胁；而从用户体验的角度，却是难以治愈的牛皮癣。在国外，它们被称为Adware（广告件）及Pornware（色情件），也统称为Spyware（间谍件）*，而在国内，它们有一个具有中国特色的名字——“流氓软件”。（注：这些比较客观的分类，都不是国人的创造。有趣的是Spyware曾被国内热炒，其实Spyware并不是指那些窃取账户密码的样本，因为那样就会被划分到Trojan（木马行列）；Spy其实指的是其进入计算机的方式是未经提示和确认的。）

而正是这种并未入传统反病毒和安全厂商法眼的轻安全威胁物种，促成了免费安全客户端的崛起。

免费对收费的超车轨迹

应该说，在免费安全客户端起事之前，反病毒是一个传统而保守的行业，采用毕其功于一役的开发方法：每年一个大版本，除了每日病毒库升级和严重Bug之外，基本不进行更新。这并非是出于懒惰，而是一个有历史原因的积习：在网络不发达的时代，反病毒产品主要是通过渠道进行基于磁盘或者光盘的分发，而病毒库升级也基本依赖拷贝完成。这使除了病毒库升级这个基础模式之外，冒然的功能改进可能产生不可预知的后果。但显然这不合乎互联网的规律。

互联网是体验的时代，很多威胁等级并不能定级到传统病毒、木马级别的“流氓软件”，给用户体验的困扰，已经远远超出了很多广泛流行的病毒、木马。

不管对反病毒产业构成了怎样的困扰，免费安全客户端在2006~2008短短两年时间内，所创造的巨大用户价值，是值得尊敬的。对“流氓软件”的坚决对抗，成了其第一个立足点。

而反病毒厂商还在被反病毒的传统技术范式困扰着，反病毒的传统模式是一个以单体文件为对象，进行匹配识别和未知检测的模型，其样本的获取依托于用户上报，和未知检测上报。而“流氓软件”是一个与普通应用软件类似的一组程序和文件，于是往往只有部分文件能被删除。

当一些资深反病毒工程师嘲笑这种删除指定目录是一种“智慧星”式的方法时，却没有意识到，这种“没有技术含量”的方法，却是实现最终用户体验的最好方法。

此时免费安全客户端尽管没有传统反病毒的底蕴，但凭借与传统厂商合作解决传统海量样本，而自身专注于“流氓软件”问题，实际已经取得了和传统反病毒软件并驾齐驱的位置。而其第二个动作——系统补丁/应用软件补丁，则开始强行超车。

从某种意义上，国内很多产业的突然兴起，都有立法缺位、企业补位的色彩，而带来的最终结果往往是越位犯规。

此事件的重要背景，是微软一度屏蔽了盗版系统的补丁能力。从传统软件厂商的意义来说，拒绝为盗版系统提供支持，或许是说得通的，特别是它们占用着正版用户的带宽支持。但落实到微软身上，却非议居多。因为这样确实使盗版比率较高的地区，安全威胁普遍泛化。

传统反病毒厂商尽管曾付出更大的代价去应对安全漏洞，他们创造过袖珍防火墙、内存补丁等很多方法。但对这种方法，他们显得保守和迟疑。他们最重要的困惑是：第三方直接从微软获取分发补丁，而不经过微软允许，是否合规。

而免费安全客户端在第三个弯道，突然开始不走寻常路，这条路叫做软件管理。对于一个以初级应用能力用户为主导的地域，还有什么能比实现软件的轻松安装更吸引人的呢？

这三个台阶并无秘密，完全可以跟进和模仿，但台阶间的粘合剂是有关厂商把用户体验挖掘到了极致。其跟踪数据、判定需求、快速改进、积极反馈形成的人/日级迭代，让一年一个大版本开发的传统反病毒软件完全脱轨。

于是，当国内传统杀毒软件厂商，奔向本场赛事终点的时候，却发现免费安全客户端的赛车已经在那里了，而车牌已经从“免费安全客户端”换成了“免费杀毒”。

所以，免费杀毒是果，有关免费客户端厂商在这个阶段竭力改善用户体验，应对和创造焦点需求才是因。尽管是传统厂商的一员，如果拒绝面对事实，我们还是会重蹈覆辙。

所以，把免费看成国内安全客户端崛起的核心原因是比较偏颇的，安全市场具有它的规律和特殊性，价格从来不是主导因素；否则国际反病毒市场的主导力量不会是传统三大厂商：赛门铁克、迈克菲和趋势，而会是AVG、AVAST等以对Home User免费为主要推广手段的厂商。

但同时，也可以非常明确地给出结论，免费安全客户端的三个崛起平台在国际市场从来不曾存在，在良好的信息安全立法和知识产权保护条件下，“流氓软件”行为受到深度的遏制；同时分发第三方产品则受到严格的限定，这三个平台确实是一个中国式图景，其本身也反映了中国在安全立法、执法和知识产权保护上的一些滞后。

商业模式的对撞

任何一个经济单元想要合理运行，必须要有其产出、收入和成本的合理模式。

无论是传统的反病毒厂商、还是以Home User免费为吸引力的半免费厂商，以及免费安全客户厂商，其实多数成本是共有的，比如研发成本、维护支持成本、推广传播成本等。免费厂商仅比收费厂商少了渠道和销售成本；但这并非是桌面安全市场的核心成本。

而传统厂商收取产品销售费用、病毒库升级费用；半免费厂商则依靠桌面免费、企业盈利；而免费安全客户端厂商靠什么盈利呢？

其实这个问题很容易找到答案，且答案令人眼花缭乱：

- **广告**：软件界面广告、依托浏览器形成的网址首页广告；
- **软件推广**：对第三方软件收费推广，包括以推广方式入股；
- **搜索引擎流量分成**：将用户操作导向搜索引擎，从搜索引擎公司获取费用；
- **网络游戏**：关联开发和代理网络游戏，提升游戏用户数；
- **销售其他杀毒软件**：早期主要盈利来源；
- **其他安全增值服务**：上门杀毒。

而在关联业务中，除了后两者，基本是和安全无关的。而由此我们可以看出，如果免费安全客户端不能在其上搭载收费的安全应用，就只能利用自身的覆盖率以及自身价值所创造的用户信任力，向互联网其他应用环

节扩展。

“用户体验、长尾价值、平台效应、唯一入口”让应用开发者奉为圭臬的，也让安全工作者不寒而栗。

但免费安全客户端的崛起、对免费魔力的膜拜，也会让这个产业进入一个不计成本、野蛮竞争的时代，秘诀只剩下一条，就是比对手付出更大的代价。你高价我低价、你收费我免费、你免费我托管代码、你托管代码我彻底开源。直到弹药耗光。

免费模式与传统安全价值观的摩擦

1999年，一位学术权威曾教导过我，“最有能力伤害安全价值观的人，就是它的捍卫者。”当时我还不理解什么是安全价值观。直到今天我还只能把它相对简单地理解成：安全产品要保护系统和数据的可用性、完整性和有效性；保护用户的知情权、选择权；安全产品要构成用户的安全边界，并要尽力避免引入新的安全威胁，等等。

而在上个月，这位老人又对我说，“如果缺少对商业原则的尊重，就不会有真正的经济文明，也就无法达成普遍的安全价值。”

那么什么又是商业原则？是契约精神吗？我突然发现商业原则、用户意愿和安全价值其实是纠结矛盾的，只是在互联网安全客户端的相关事件中爆发了。

比如网络门户，让我们不用购买报纸而知安全天下事，但不买报纸的代价是无法避免地看到广告链接和弹窗，这个代价与所得其实是一个商业契约。但用户希望遵守这个契约吗？显然多数用户并不情愿。安全软件封杀门户弹窗是符合多数用户意愿的，但安全软件有破坏第三方商业契约的权利吗？

类似的疑惑很多，如果作为收费的安全软件，在界面上推荐一款网络游戏是否算引入安全威胁，我会毫不犹豫的回答——是！但免费安全工具的使用，本身就是用户选择的契约行为。契约本身又是需要尊重的，那么是否是安全价值观出错了呢？似乎也没有。

又如我确实认为“恶评软件”是一个比“流氓软件”更精彩的商业创意，当传统厂商面对被查杀插件厂商的律师函无计可施的时候，免费安全客户端厂商确实无比精明地把裁决权交给了“网民”。但时隔多年反思，当公众曾为民意查杀而叫好的时候，却没有注意到民意的表达只是数据库的数字，而无法监督其形成过程。当然，我们不怀疑同行的操守，但如果一个合法而优秀的应用工具，可以被投票刷成恶评软件，又该如何处理呢？

这不是更可怕的，更可怕的是，假如赋予一款安全软件不依据技术规范和标准来清除某个插件的权利，他其实同时也拥有了另外一项权利，即不杀的权利。这是一个令人不敢推演和想象的轨迹。

但有一点我毫不顾虑地坚持：对于社会的全局安全来说，安全环节的多样性是一个重要的前提，如果全世界的防盗门都是一个品牌，那基本就等于没有防盗门。

由于反病毒的核心方法是基于海量规则（已知检测）和预设模型（未知检测）的机制，而其先天软肋在于它是一种易于获得的、可以被攻击方反复测试绕过的资源。因此如果产品过于单一，其全局安全的系数就会下降。

所以免费安全客户端，是一个新的物种，生活在操作系统草原和互联网星空之间，采用着传统安全软件的技术，和我们这些传统厂商一样处置着恶意代码，它们保障着但似乎也威慑着应用软件的价值。

我承认它们创造过的价值，但如果他们的翅膀遮蔽了星空，我会保持警惕。

结束语

不管是接受还是排斥，免费安全客户端在中国互联网已居于桌面安全主导地位。而依然坚持销售路线的桌面反病毒软件的传统厂商们讶异地发现，无论它们还保有怎样的装机量，甚至依然不俗的业绩，在舆论、公众认知眼中，它们都不再是城市英雄，而居于配角地位。由于免费客户端的平台媒体效应，它们基本失去了话语权。

最可怕的对手，不是采用同一个规则和你打得你死我活的对手，而是和你完全行走不同规则的对手。当对抗完全处于不对称，就会造成一边倒的倾覆。

最惨烈的竞争，则一定发生于相同游戏规则的竞技者之间：免费安全客户端的竞争对手必然是以客户端模式为主导的互联网应用。所以今后我们看到更多的将是，免费应用和免费安全之间的频繁摩擦。免费安全为了解决没有盈利模式的尴尬，会努力地向“免费”应用扩展，而免费应用为了自保和制衡，会不断地自行扩展安全关联环节。

对于一个保守而传统的反病毒工作者来说，只有一个敌人，那就是病毒。但如果在反病毒对抗之外，还有一个充满产业乱象战场的话，我相信，那个战场会有更多有热忱梦想的人加入，也会有更多崇尚安全价值的人远离。

而如果跳开单点的矛盾和纠结来看，产业秩序才是产业的最大正义。这也决定了必然会有很多人为良性的产业秩序而斗争。